Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-50 (Cancelled)

51. (Allowed) A data transfer method performed by a proxy server, the method comprising:

intercepting an HTTP request from a client computer that is directed to an HTTP server, wherein the HTTP request comprises a plurality of fields;

determining an identity of a user of the client computer in response to receiving the HTTP request;

accessing a storage associated with the proxy server, the storage storing identifiers for use by HTTP servers in retrieving user profile information stored in storages associated with the HTTP servers;

retrieving an identifier from the accessed storage based on the identity of the user;

inserting an additional field into the HTTP request to create a modified HTTP request, the additional field containing the retrieved identifier;

sending the modified HTTP request to the HTTP server such that the HTTP server parses the modified HTTP request to extract the retrieved identifier, uses the retrieved identifier to retrieve the user profile information from a storage associated with the HTTP server, generate an HTTP response to the HTTP request based on the retrieved user profile information, and sends the HTTP response to the proxy server;

receiving the HTTP response from the HTTP server; and

forwarding the HTTP response to the client computer.

52. (Currently Amended) The method of claim 51 further comprising:

receiving an initial HTTP request from the client computer that is directed to the HTTP server, wherein the initial HTTP request comprises a plurality of fields;

determining an identity of a user of the client computer in response to receiving the initial HTTP request;

retrieving user profile information based on the identity of the user;

encrypting the user profile information;

inserting an additional field into the initial HTTP request to create a modified initial HTTP request, wherein the additional field inserted into the initial HTTP request contains the encrypted user profile information;

sending the modified initial HTTP request to the HTTP server such that the HTTP server parses the modified initial HTTP request to extract and decrypt the encrypted user profile information, stores the decrypted user profile information in the storage associated with the HTTP server, generates an initial HTTP response to the initial HTTP request based on the decrypted user profile information, generates the identifier, and sends the initial HTTP response and the identifier to the proxy server;

receiving the identifier from the HTTP server;

storing the identifier in the storage associated with the proxy server;

receiving the initial HTTP response from the initial HTTP server; and

forwarding the initial HTTP response to the client computer.

53. (Allowed) The method of claim 52 wherein encrypting the user profile information comprises determining a session key and using the session key to encrypt the user profile information.

54. (Allowed) The method of claim 53 further comprising:

encrypting the session key; and

inserting a second additional field into the initial HTTP request to create the modified initial HTTP request, wherein the second additional field inserted into the initial HTTP request contains the encrypted session key.

55. (Allowed) The method of claim 54 wherein:

using the session key to encrypt the profile information comprises using the session key and a symmetric encryption algorithm to encrypt the user profile information, and

encrypting the session key comprises encrypting the session key using a public key encryption algorithm and a public key associated with the HTTP server.

56. (Allowed) The method of claim 55 further comprising obtaining the public key from the HTTP server.

57. (Allowed) The method of claim 56 wherein obtaining the public key from the HTTP server comprises sending a request to the HTTP server to retrieve the public key.

58. (Allowed) The method of claim 53 wherein determining the session key comprises combining a master session key with a key mask.

59. (Allowed) The method of claim 51 wherein determining the identity of the user comprises:

determining an IP address of the client computer; and

querying a database to determine an identity associated with the IP address in the database.

60. (Allowed) The method of claim 52 further comprising determining that the HTTP server should receive the user profile information.

61. (Allowed) The method of claim 60 wherein determining that the HTTP server should receive the user profile information includes querying a database associated with the proxy server to determine if the HTTP server should receive the user profile information.

62. (Allowed) The method of claim 51 wherein determining the identity of the user comprises using the Internet Engineering Task Force IDENT protocol to determine the identity of the user.

63. (Allowed) The method of claim 51 wherein the user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

64. (Currently Amended) The method of claim 51 further comprising sending a flush directive to the HTTP server such that the HTTP server discards the user profile information stored in the storage associated with the HTTP server.

65. (Allowed) A data processing method performed by an HTTP server, the method comprising:

receiving a modified HTTP request from a proxy server, wherein the proxy server created the modified HTTP request by inserting a field into an HTTP request intercepted by the proxy server, the inserted field containing an identifier;

parsing the modified HTTP request to extract the identifier;

using the extracted identifier to retrieve user profile information from a storage associated with the HTTP server;

generating an HTTP response to the HTTP request based on the retrieved user profile information; and

sending the HTTP response to the proxy server for delivery to a client computer.

66. (Allowed) The method of claim 65 further comprising:

receiving an initial modified HTTP request from a proxy server, wherein the initial modified HTTP request includes a field inserted into an initial HTTP request by the proxy server, wherein the field inserted into the initial HTTP request contains encrypted user profile information;

parsing the initial modified HTTP request to extract the encrypted user profile information;

decrypting the encrypted user profile information extracted from the initial modified HTTP request;

generating an initial HTTP response to the initial HTTP request based on the decrypted user profile information;

sending the initial HTTP response to the proxy server for delivery to a client computer;

storing the decrypted user profile information in the storage associated with the HTTP server;

generating the identifier; and

sending the identifier to the proxy server.

67. (Allowed) The method of claim 66 wherein generating an initial HTTP response to the initial HTTP request based on the decrypted user profile information comprises providing the decrypted user profile information to a web application.

68. (Allowed) The method of claim 67 wherein the web application comprises a common gateway interface script and providing the decrypted user profile information to the web application comprises setting HTTP environment variables accessible to the common gateway interface script.

69. (Currently Amended) The method of claim 66 wherein

the initial modified HTTP request includes a second field inserted into the initial HTTP request by the proxy server, wherein the second field inserted into the initial HTTP request contains a session key, and

decrypting the encrypted user profile information comprises decrypting the encrypted user profile information extracted from the initial modified HTTP request using the session key.

70. (Allowed) The method of claim 69 further comprising decrypting the session key.

71. (Allowed) The method of claim 70 wherein:

decrypting the session key comprises decrypting the session key using a public key algorithm and a private key of the HTTP server, and

decrypting the encrypted user profile information using the session key comprises decrypting the encrypted user profile information using a symmetric decryption algorithm and the session key.

72. (Allowed) The method of claim 65 wherein the user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

73. (Allowed) The method of claim 65 further comprising:

receiving a flush directive from the proxy server; and

in response to receiving the flush directive, discarding the user profile information stored in the local storage.

74. (Allowed) A computer-usable medium having a computer program embodied thereon, the computer program comprising instructions for causing a proxy server to:

intercept an HTTP request from a client computer that is directed to an HTTP server, wherein the HTTP request comprises a plurality of fields;

determine an identity of a user of the client computer in response to receiving the HTTP request;

access a storage associated with the proxy server, the storage storing identifiers for use by HTTP servers in retrieving user profile information stored in storages associated with the HTTP servers;

retrieve an identifier from the accessed storage based on the identity of the user;

insert an additional field into the HTTP request to create a modified HTTP request, the additional field containing the retrieved identifier;

send the modified HTTP request to the HTTP server such that the HTTP server parses the modified HTTP request to extract the retrieved identifier, uses the retrieved identifier to retrieve user profile information from a storage associated with the HTTP server, generate an HTTP response to the HTTP request based on the retrieved user profile information, and sends the HTTP response to the proxy server;

receive the HTTP response from the HTTP server; and

forward the HTTP response to the client computer.

75. (Currently Amended) The medium of claim 74 wherein the computer program further comprises instructions for causing the proxy server to:

receive an initial HTTP request from the client computer that is directed to the HTTP server, wherein the initial HTTP request comprises a plurality of fields;

determine an identity of a user of the client computer in response to receiving the initial HTTP request;

retrieve user profile information based on the identity of the user;

encrypt the user profile information;

insert an additional field into the initial HTTP request to create a modified initial HTTP request, wherein the additional field inserted into the initial HTTP request contains the encrypted user profile information;

send the modified initial HTTP request to the HTTP server such that the HTTP server parses the modified initial HTTP request to extract and decrypt the encrypted user profile information, stores the decrypted user profile information in the storage associated with the HTTP server, generates an initial HTTP response to the initial HTTP request based on the decrypted user profile information, generates the identifier, and sends the initial HTTP response and the identifier to the proxy server;

receive the identifier from the HTTP server;

store the identifier in the storage associated with the proxy server;

receive the initial HTTP response from the initial HTTP server; and

forward the initial HTTP response to the client computer.

76. (Allowed) The medium of claim 75 wherein, to encrypt the user profile information, the computer program further comprises instructions for causing the proxy server to determine a session key and using the session key to encrypt the user profile information.

77. (Allowed) The medium of claim 76 wherein the computer program further comprises instructions for causing the proxy server to:

encrypt the session key; and

insert a second additional field into the initial HTTP request to create the modified initial HTTP request, wherein the second additional field inserted into the initial HTTP request contains the encrypted session key.

78. (Allowed) The medium of claim 77 wherein:

to use the session key to encrypt the profile information, the computer program further comprises instructions for causing the proxy server to use the session key and a symmetric encryption algorithm to encrypt the user profile information, and

to encrypt the session key, the computer program further comprises instructions for causing the proxy server to encrypt the session key using a public key encryption algorithm and a public key associated with the HTTP server.

79. (Allowed) The medium of claim 76 wherein, to determine the session key, the computer program further comprises instructions for causing the proxy server to combine a master session key with a key mask.

80. (Allowed) The medium of claim 74 wherein the user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

81. (Currently Amended) The medium of claim 74 wherein the computer program further comprises instructions for causing the proxy server to send a flush directive to the HTTP server such that the HTTP server discards the user profile information stored in the storage associated with the HTTP server.

82. (Allowed) A computer-usable medium having a computer program embodied thereon, the computer program comprising instructions for causing an HTTP server to:

receive a modified HTTP request from a proxy server, wherein the proxy server created the modified HTTP request by inserting a field into an HTTP request intercepted by the proxy server, the inserted field containing an identifier;

parse the modified HTTP request to extract the identifier;

use the extracted identifier to retrieve user profile information from a storage associated with the HTTP server;

generate an HTTP response to the HTTP request based on the retrieved user profile information; and

send the HTTP response to the proxy server for delivery to a client computer.

83. (Allowed) The medium of claim 82 wherein the computer program further comprises instructions for causing the HTTP server to:

receive an initial modified HTTP request from a proxy server, wherein the initial modified HTTP request includes a field inserted into an initial HTTP request by the proxy server, wherein the field inserted into the initial HTTP request contains encrypted user profile information;

parse the initial modified HTTP request to extract the encrypted user profile information;

decrypt the encrypted user profile information extracted from the initial modified HTTP request;

generate an initial HTTP response to the initial HTTP request based on the decrypted user profile information;

send the initial HTTP response to the proxy server for delivery to a client computer;

store the decrypted user profile information in the storage associated with the HTTP server;

generate the identifier; and

send the identifier to the proxy server.

84. (Allowed) The medium of claim 83 wherein

the initial modified HTTP request includes a second field inserted into the initial HTTP request by the proxy server, wherein the second field inserted into the initial HTTP request contains a session key, and

to decrypt the encrypted user profile information, the computer program further comprises instructions for causing the HTTP server to decrypt the encrypted user profile information extracted from the initial modified HTTP request using the session key.

85. (Allowed) The medium of claim 84 wherein the computer program further comprises instructions for causing the HTTP server to decrypt the session key.

86. (Allowed) The medium of claim 85 wherein:

to decrypt the session key, the computer program further comprises instructions for causing the HTTP server to decrypt the session key using a public key algorithm and a private key of the HTTP server, and

to decrypt the encrypted user profile information using the session key, the computer program further comprises instructions for causing the HTTP server to decrypt the encrypted user profile information using a symmetric decryption algorithm and the session key.

87. (Allowed) The medium of claim 82 wherein the user profile information comprises one or more of demographic information, a history of data requests by a user, age of a user, gender of a user, or interests of a user.

88. (Allowed) The medium of claim 82 wherein the computer program further comprises instructions for causing the proxy server to:

receive a flush directive from the proxy server; and

discard the user profile information stored in the local storage.

89. (Allowed) A proxy server comprising:

a storage to store identifiers for use by HTTP servers in retrieving user profile information stored in storages associated with the HTTP servers;

a network interface operatively coupled to a network to exchange data with a client computer and with the HTTP server; and

a processor operatively coupled to the network interface, the storage, and a memory comprising executable instructions for causing the processor to:

intercept an HTTP request from a client computer that is directed to an HTTP server, wherein the HTTP request comprises a plurality of fields;

determine an identity of a user of the client computer in response to receiving the HTTP request;

retrieve an identifier from the storage based on the identity of the user;

insert an additional field into the HTTP request to create a modified HTTP request, the additional field containing the retrieved identifier;

send the modified HTTP request to the HTTP server such that the HTTP server parses the modified HTTP request to extract the retrieved identifier, uses the retrieved identifier to retrieve user profile information from a storage associated with the HTTP server, generate an HTTP response to the HTTP request based on the retrieved user profile information, and sends the HTTP response to the proxy server;

receive the HTTP response from the HTTP server; and

forward the HTTP response to the client computer.

90. (Currently Amended) The proxy server of claim 89 wherein the memory further comprises executable instructions for causing the processor to:

receive an initial HTTP request from the client computer that is directed to the HTTP server, wherein the initial HTTP request comprises a plurality of fields;

determine an identity of a user of the client computer in response to receiving the initial HTTP request;

retrieve user profile information based on the identity of the user;

encrypt the user profile information;

insert an additional field into the initial HTTP request to create a modified initial HTTP request, wherein the additional field inserted into the initial HTTP request contains the encrypted user profile information;

send the modified initial HTTP request to the HTTP server such that the HTTP server parses the modified initial HTTP request to extract and decrypt the encrypted user profile information, stores the decrypted user profile information in the storage associated with the HTTP server, generates an initial HTTP response to the initial HTTP request based on the decrypted user profile information, generates the identifier, and sends the initial HTTP response and the identifier to the proxy server;

receive the identifier from the HTTP server;

store the identifier in the storage associated with the proxy server;

receive the initial HTTP response from the HTTP server; and

forward the initial HTTP response to the client computer.

91. (Allowed) The proxy server of claim 90 wherein, to encrypt the user profile information, the memory further comprises executable instructions for causing the processor to determine a session key and using the session key to encrypt the user profile information.

92. (Allowed) The proxy server of claim 91 wherein the memory further comprises executable instructions for causing the processor to:

encrypt the session key; and

insert a second additional field into the initial HTTP request to create the modified initial HTTP request, wherein the second additional field inserted into the initial HTTP request contains the encrypted session key.

93. (Allowed) The proxy server of claim 92 wherein:

to use the session key to encrypt the profile information, the memory further comprises executable instructions for causing the processor to use the session key and a symmetric encryption algorithm to encrypt the user profile information, and

to encrypt the session key, the memory further comprises executable instructions for causing the processor to encrypt the session key using a public key encryption algorithm and a public key associated with the HTTP server.

94. (Allowed) The proxy server of claim 91 wherein, to determine the session key, the memory further comprises executable instructions for causing the processor to combine a master session key with a key mask.

95. (Allowed) An HTTP server comprising:

a storage to store user profile information;

a network interface operatively coupled to a network to exchange data with a proxy server; and

a processor operatively coupled to the network interface and a memory comprising executable instructions for causing the processor to:

receive a modified HTTP request from a proxy server, wherein the proxy server created the modified HTTP request by inserting a field into an HTTP request intercepted by the proxy server, the inserted field containing an identifier;

parse the modified HTTP request to extract the identifier;

use the extracted identifier to retrieve user profile information from the storage;

generate an HTTP response to the HTTP request based on the retrieved user profile information; and

send the HTTP response to the proxy server for delivery to a client computer.

96. (Allowed) The HTTP server of claim 95 wherein the memory further comprises executable instructions for causing the processor to:

receive an initial modified HTTP request from a proxy server, wherein the initial modified HTTP request includes a field inserted into an initial HTTP request by the proxy server, wherein the field inserted into the initial HTTP request contains encrypted user profile information;

parse the initial modified HTTP request to extract the encrypted user profile information;

decrypt the encrypted user profile information extracted from the initial modified HTTP request;

generate an initial HTTP response to the initial HTTP request based on the decrypted user profile information;

send the initial HTTP response to the proxy server for delivery to a client computer;

store the decrypted user profile information in the storage;

generate the identifier; and

send the identifier to the proxy server.

97. (Allowed) The HTTP sever of claim 96 wherein

the initial modified HTTP request includes a second field inserted into the initial HTTP request by the proxy server, wherein the second field inserted into the initial HTTP request contains a session key, and

to decrypt the encrypted user profile information, the memory further comprises executable instructions for causing the processor to decrypt the encrypted user profile information extracted from the initial modified HTTP request using the session key.

98. (Allowed) The HTTP server of claim 97 wherein the memory further comprises executable instructions for causing the processor to decrypt the session key.

99. (Allowed) The HTTP server of claim 98 wherein:

to decrypt the session key, the memory further comprises executable instructions for causing the processor to decrypt the session key using a public key algorithm and a private key of the HTTP server, and

to decrypt the encrypted user profile information using the session key, the memory further comprises executable instructions for causing the processor to decrypt the encrypted user profile information using a symmetric decryption algorithm and the session key.